AFFIDAVIT OF MICHAEL AGOSTINHO

1. I am a Special Agent with United States Department of Homeland Security, Immigrations and Customs Enforcement, Homeland Security Investigations ("HSI") and am assigned to the office of the Resident Agent in Charge, Providence, Rhode, Island. I have been an HSI agent since 2008. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, including violations of 18 U.S.C. §§ 2422, 2251, 2252, and 2252A. I have received training in the investigation of child pornography, child exploitation, and transportation of minors, and have reviewed examples of child pornography as specified in 18 U.S.C. § 2256.

2. I submit this affidavit in support of a warrant to search the computer device described in Attachment A, which is Brian Murphy's Apple iPad A2200 (serial number DMPCMCNEMDG1) (hereinafter, the "Device") for records as specified in Attachment B.

3. The information in this affidavit is based my personal observations and investigation, my training and experience, and information provided by others, including law enforcement officers, probation officers, the National Center for Missing and Exploited Children ("NCMEC"), and Kik. This affidavit does not set forth the totality of my knowledge about this matter or investigation. I set forth here only the facts that I believe are necessary to assess and establish probable cause.

4. As described below, there is probable cause to believe that Brian Murphy (born in October 1969) (hereinafter "Murphy") used the Device to receive, view, and distribute child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (a)(4). Based on the use of the Device, there is also probable cause to believe that it is an instrumentality of the aforementioned offenses and contains evidence of those

offenses and fruit of those offenses, namely images and/or videos constituting child pornography.

Probable Cause

5. In or around April 2022, NEMEC advised members of the Rhode Island Crimes against Children Task Force ("ICAC") that security personnel associated with Kik (a company that operates a mobile messaging application for chat communications, group chat communications, and the transmissions and receipt of messages, videos, pictures, and gifs) had in March 2022 become aware that an individual utilizing a Kik messenger account associated with user name "bialexdad" had uploaded 151 files containing child pornography and child erotica, using IP address 68.15.57.11. Those 151 files are presently in the custody of the ICAC.

6. Warwick Detective Patrick Smith, a member of the ICAC, examined some of the 151 files. One of the files is a video depicting a nude prepubescent female lying on her back being anally penetrated by a penis.

7. Detective Smith, through an inquiry with the American Registry of Internet Numbers, determined that the aforementioned IP address was utilized by Cox Communications. After legal process was issued, Cox Communications reported that the aforementioned IP address was associated with a business located at 138 Danielson Pike in North Scituate. Detective Smith, in July 2022, traveled to the address and found a multi-family building there with the business identified by Cox on the ground floor. The business was a coffee shop that provided Wi-Fi internet access for its customers. Detective Smith noticed that the units above the coffee shop were consistent with apartments.

8. According to tax assessor records, the building that houses the coffee shop is a mixed-use commercial building with units bearing addresses that include 138 Danielson Pike and 136 Danielson Pike. According to law enforcement

databases, Murphy is registered as a Federal Level II sex offender and is listed as residing at 136 Danielson Pike, Unit 2, North Situate, RI 02857.

9. I know based on my training and experience and use of Wi-Fi services at retail stores and coffee shops that it is not uncommon for Wi-Fi signals to reach beyond the confines of such stores or shops and that in a typical multi-family building with such a store or shop on the ground floor, it would not be uncommon for those who reside in the apartments above to be able to utilize computer devices to access the internet using the store's Wi-Fi signal.

10. Murphy was in 2009 convicted in this district on federal charges of possession and distribution of pornography and sentenced to 84 months of incarceration followed by a lifetime of supervised release. That case is docketed at 09-CR-0058-S. That case was the product of an HSI investigation, and I have reviewed case reports from that investigation. According to those reports, Murphy exchanged child pornography files with others utilizing a social media application named "Hello[,]" and his Hello account user name was "bidaddy69[,]" a name similar "bialexdad[,]" which is the user name for the Kik account that uploaded, according to Kik, 151 files containing child pornography.

10. U.S. Probation Officer Anthony Desjardin was apprised of the above described NECMEC referral, IP-address tie to the coffee shop, Murphy's proximity to the coffee shop and its Wi-Fi service, and the similarity of the user names. Based on this information, the Probation Department, accompanied by HSI agents and other law enforcement officers, opted to search Murphy's person, property, and computer device pursuant to the reasonable suspicion search condition that was ordered as part of Murphy's supervised release. That condition reads as follows:

> "The defendant submit to a search of his person, property house, residence, vehicle, papers, computer, or other electronic communication or data storage devices or media, and effects at any time, with or without a warrant,

> by any law enforcement or probation officer with reasonable suspicion concerning unlawful conduct or a violation of a condition of supervised release."

11. On the morning of August 24, 2022, Probation Officer Desjardin approached Murphy as he was walking toward his car, which was parked in a parking area next to the multi-family building that houses Murphy's apartment, and the two spoke. Desjardin advised that he intended to conduct a reasonable suspicion search of Murphy's residence and car and that law enforcement agents were accompanying him. In the course of conversation, Murphy admitted that he had being viewing child pornography on a work "laptop."

12. Inside his residence, after being advised of his *Miranda* rights, Murphy told law enforcement agents that the computer was in his bedroom. Agents found the Device in the bedroom closet and placed it into airplane mode. On cursory examination of the Device, multiple images of child pornography were found. One particular image, which was located in an application entitled "Wickr Me," was sent from the Device using the account name "bialexdad" to a chat room entitled "♥CP♥♥SHARE HERE♥♥N.L♥Tab00♥[.]" This image depicted two prepubescent males engaged in oral sex with one another and was sent on August 20, 2022 at 11:04 am. There were also several other images being sent and received in that chat room and others within the Wickr Me application.

13. After Murphy had been *Mirandized*, I spoke to him. He made the following admissions:

- he admitted to using his work computer to view child pornography and identified the Device as his work computer,
- he admits to using the coffee shop's Wi-Fi since he moved into his apartment, and he indicated that he had been living in his apartment for approximately 4 years,

- he admitted that on the WickR application he uses the user name "bialexdad[,]"
- he said that he only used the Device for viewing child pornography,
- he admitted that he both electronically send and received child pornography using a variety of social media application, including WickR,
- he said that his preferred child pornography age is 12, and
- he admitted that he understood what child pornography was and that he used it for masturbation and sexual gratification purposes.

Technical Terms and the Device

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos. I note that iPads, including the seized Device, have built in digital cameras.

b. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for

example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks. I note that iPads, including the seized Device, are tablets.

c. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

15. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a digital camera, a tablet, and a device capable of connecting to the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

Probable Cause to Search the Device

16. During the course of the search of Murphy's apartment, the Device was seized and is presently in the custody of the ICAC. It was seized by the ICAC for preservation of its contents as evidence, after the above-described reasonable suspicion search revealed, on cursory examination, that the Device contained items of child pornography under circumstances indicating that they had been possessed, received, and distributed. There is accordingly, probable cause to believe that a

more thorough examination of the device would reveal the already found child pornography as well as additional child pornography and correspondence of communication relating to receipt and distribution.

17. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

18. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating

system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion

is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to receive and distribution child pornography, the individual's electronic device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

22. *Manner of execution.* Because this warrant seeks only permission to examine a Device already in law enforcement's possession, the execution of this

warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

14. Based on the foregoing, I believe that there is probable cause to believe that the Device is an instrumentality and contains evidence and fruits of possession, receipt and distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2) and (a)(4), and that there is proable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Michael Agostinho
HSI Special Agent

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by **Telephone**.

(specify reliable electronic means)

August 26, 2022

Date | *Judge's signature*

Providence RI | Lincoln D Almond USMJ

City and State | *Printed name and title*

ATTACHMENT A

THING TO BE SEARCHED

One Apple iPad A2200 (serial number DMPCMCNEMDG1) found on August 24, 2022 in the residence of Brian Murphy at 136 Danielson Pike, Unit 2, North Situate, RI 02857, herein after the "Device." The Device is presently in the custody of the Rhode Island Crimes against Children Task Force.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information. described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 2252(a)(2) and involve Brian Murphy since January 1, 2018, including:

a. images or videos constituting child pornography, obscenity, or child erotica,

b. records or information relating to the distribution, receipt, or possession of child pornography, obscenity, or child erotica,

c. records or information relating to efforts to disguise, cloak, or conceal the distribution, receipt, or possession of child pornography, obscenity, or child erotica,

d. records or information relating to use of Kik, WickR, Wickr Me, WickR Me, or any other social media application for the distribution, receipt, or possession of child pornography, obscenity, or child erotica,

e. records or information relating to communications with minors or others having access to minors for the purpose of obtaining or creating child pornography, obscenity, or child erotica,

f. records or information relating to the identity of the user or utilizer of user name "bialexdad" and/or "bidaddy69,"

g. evidence of computer software that would allow others to control the items, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software,

h. evidence of the attachment of other computer hardware or storage media,

i. evidence of counter forensic programs and associated data that are designed to eliminate data,

j. evidence of the times that the Device was used,

k. passwords, encryption keys, and other access devices that may be necessary to access or use the Device or applications on the Device,

l. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media, and

m. evidence indicating the computer user's state of mind as it relates to the crime under investigation.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the Internet Protocol address 68.15.57.11 or any Internet Protocol address associated with Wi-Fi service provided by a retail establishment, such as a coffee shop, including:

a. records of Internet Protocol addresses used, and

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

5. For the purpose of this warrant:

a. "Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, cellular telephone, or wireless

communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

b. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

c. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

d. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

e. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

f. “Obscene material” is any image or video representation containing material which the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; depicts in a patently offensive way, sexual conduct and taken as a whole, lacks serious literary, artistic, political, or scientific value such as patently offensive representations or descriptions of ultimate sexual acts, normal or perverted, actual or simulated, patently offensive representation or descriptions of masturbation, excretory functions, and lewd exhibition of the genitals.